腾讯音乐娱乐 酷狗音乐

# 谈Google“零信任”模型的基础安全架构

BeyondCorp基础安全架构解析

# 目录

# 基础安全的历史与现状

斯巴达密码棒（古代）

防火墙、特权网络（中世纪）

安全运营中心（SOC）（近代）

安全运作和分析平台（ SOAPA ）（现代）

# BeyondCorp目标设定

- 让所有Google员工从不受信任的网络中不接入VPN就能顺利工作。

# 威胁案例

- 看我如何进入并且漫游京东内网
- 重庆市民政局敏感信息泄漏已进入VPN应用系统

- 看我如何用wifi万能钥匙物理撸穿京东漫游内网

- 苹果Xcode后门事件
- putty、xshell后门事件

# Github 关键信息泄露

```
#\u90AE\u7BB1\u53D1\u9001\u914D\u7F6E
mail.from=baihua@kugou.com
mail.host=smtp.qiye.163.com
mail.username=baihua@kugou.com
mail.password=Bigao20152016
mail.encoding=UTF-8
#\u90AE\u7BB1\u7AEF\u53E3\u53F7
mailserver.port=5025
money=true
#\u7CFB\u7EDF\u5185\u90E8\u5F02\u5E38\u53D1\u90AE\u4EF6\u7ED9\u5F00\u53D1\u8005
send_error_to_coder=true
coder_email=su1989hai@126.com

show_response=true
show_request=true
```

```
#qq\u7684appId
qq_app_id=1105673196
#\u9177\u72D7\u767B\u5F55
ku_gou_login_url=
ku_gou_third_login_url
ku_gou_app_id=2101
ku_gou_app_key=ulSwMbWxmyFb1MU4mLFxtvSPzeJh6xPL
user_default_img_url=http://ds.baihua.kugou.com/static/images/img_default.png

redis.servers=192.168.7.218:7000,192.168.7.219:7000,192.168.7.219:7001

#\u90AE\u7BB1\u53D1\u9001\u914D\u7F6E
```

# 关键信息泄露

```
kugouVpnHost    += "###Kugou_Vpn_Hosts_Begin\r\n";
kugouVpnHost    += "10.16.4.182 rtx.kugou.com\r\n";
kugouVpnHost    += "10.16.2.65  oa.kugou.net\r\n";
kugouVpnHost    += "10.16.2.65  opd.kugou.net\r\n";
kugouVpnHost    += "10.16.2.65  qa.kugou.net\r\n";
kugouVpnHost    += "10.16.2.65  kgedit2.kugou.com\r\n";
kugouVpnHost    += "172.17.13.71    mtp.kugou.net\r\n";
kugouVpnHost    += "10.12.0.85  mail.kugou.net\r\n";
kugouVpnHost    += "10.16.4.45  pms.kugou.com\r\n";
kugouVpnHost    += "10.16.6.198 cost.tencentmusic.com\r\n";
kugouVpnHost    += "10.12.0.85  autodiscover.kugou.net\r\n";
kugouVpnHost    += "10.16.2.65  musiclib.admin.kugou.com\r\n";
kugouVpnHost    += "10.16.2.65  topic.5sing.kugou.net\r\n";
kugouVpnHost    += "10.16.2.65  kgedit2.kugou.com\r\n";
kugouVpnHost    += "10.16.2.65  bi.kugou.com\r\n";
kugouVpnHost    += "10.12.0.85  mail.kugou.net\r\n";
kugouVpnHost    += "10.16.2.25  svn.kugou.net\r\n";
kugouVpnHost    += "172.17.13.71    mtp.kugou.net\r\n";
kugouVpnHost    += "10.12.0.2   bi.kugou.net\r\n";
kugouVpnHost    += "10.16.2.65  biadmin.kugou.net\r\n";
kugouVpnHost    += "10.16.2.65  rt.manage.kugou.com\r\n";
kugouVpnHost    += "10.16.2.65  tp.kugou.net\r\n";
kugouVpnHost    += "10.16.4.129  test-kgmedit.kugou.com\r\n";
kugouVpnHost    += "10.16.4.129  kgmedittest.kugou.com\r\n";
kugouVpnHost    += "###Kugou_Vpn_Hosts_end\r\n";
```

```
        versionUpdateUrl: 'https://qywx.kugou.com/vpn/update.php',
        versionUpdatePath: 'https://qywx.kugou.com/vpn/download.php',
        salt: "hlkerlerer?wew9s82!",
        isCheckedConfig: false,
        configFileName: '',
        ticketData: null,
        connectType: 'account',
        loginTime: null, //登录时间
        loginTimeout: 14390, //断开时间
    },
    methods: {
        connectVpn: function(){...
        },
        handleConnectVpn: function(index) {...
        },
        encryptPassword: function(data, type) {
            data = data + "-" + app.appVersion + "-" + process.platform;
            data = data + '-' + app.salt;
            data = data + '-' + type;
            data = data.split("").reverse().join("");
            return data;
        },
        deleteLogFile: function() {
```

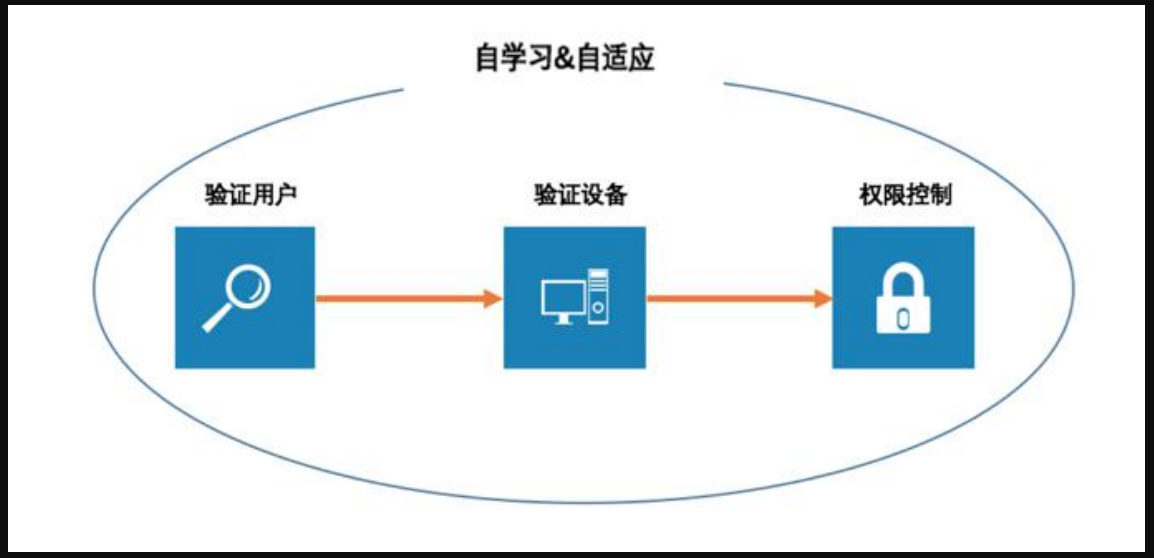
# BeyondCorp的背景

- 安全边界的概念已经难以适应今天的网络环境；
- 内部人员的误操作和恶意破坏（Insider Threat，内部人威胁）一直是企业安全的巨大挑战；
- 云计算的发展，不但原本建立的内外边界变得模糊，传统的边界安全体系对用户在外部网络直接访问公有云服务更是完全无能为力。

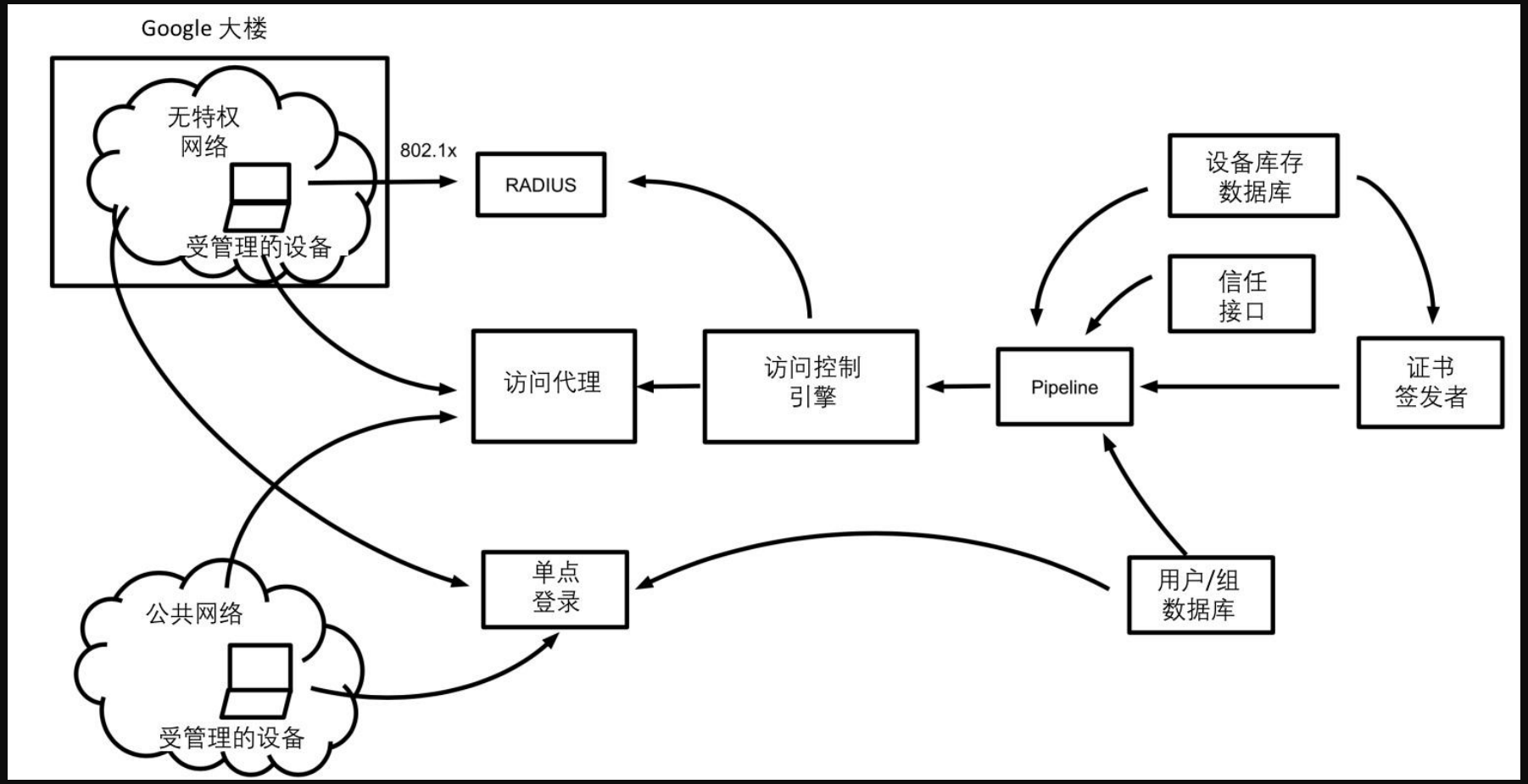
# BeyondCorp计划解析



- 谷歌的BeyondCorp计划打造基于“零信任”模型的网络安全基础架构，认证基于守信任的设备和用户而非网络本身。
- 通过中心化的认证、授权和访问控制系统，从而真正彻底改变了企业的安全体系



# BeyondCorp组件和访问流程



# 架构模块描述-安全设备识别

- 设备清单数据库
  - “受控设备”的概念—谷歌会追踪设备发生的变化，这些信息会被监控、分析。
- 设备标识
  - 唯一标识用于索引设备清单数据库，只有设备状态和信息正确才可以获得证书。

# 架构模块描述-安全识别用户



- 用户和群组数据库
  - 用于追踪和管理用户和群组中所有用户，与HR流程集成会根据岗位分类、用户名和群组成员关系紧密集成。
- 单点登录系统（SSO）
  - 外化的单点登录系统，用户进行双因子认证，通过合法验证后，SSO生成短时令牌。

# 架构模块描述-从网络中消除信任

- 部署无特权网络
  - 无特权网络只能连接互联网、有限的基础设施服务（如DNS、DHCP）
- 有线和无线网络接入的802.1x认证
  - 通过802.1x认证的RADIUS服务器实现动态的VLAN分配。
  - 如无法识别或者非受控设备会被分配到补救网络或访客网络中。

# 架构模块描述-外化应用和工作流



- 面向互联网的访问代理
  - 所有企业应用通过一个面向互联网的代理开放给外部和内部客户，通过访问代理，客户端和应用之间的流量被强制加密。
- 公共的DNS记录
  - 企业对外所有服务注册到公共DNS，使用CNAME指向到访问代理。

# 架构模块描述-实现基于清单的访问控制



- 对设备和用户的信任推断
  - 用户和设备的访问级别可能随时改变。
- 访问控制引擎
  - 代理中心通过访问控制引擎，对每个请求为企业应用提供服务级的授权。
- 访问控制引擎的消息管道
  - 通过消息管道向控制引擎推送信息，动态实时的对访问控制决策有用的信息。

# 小结

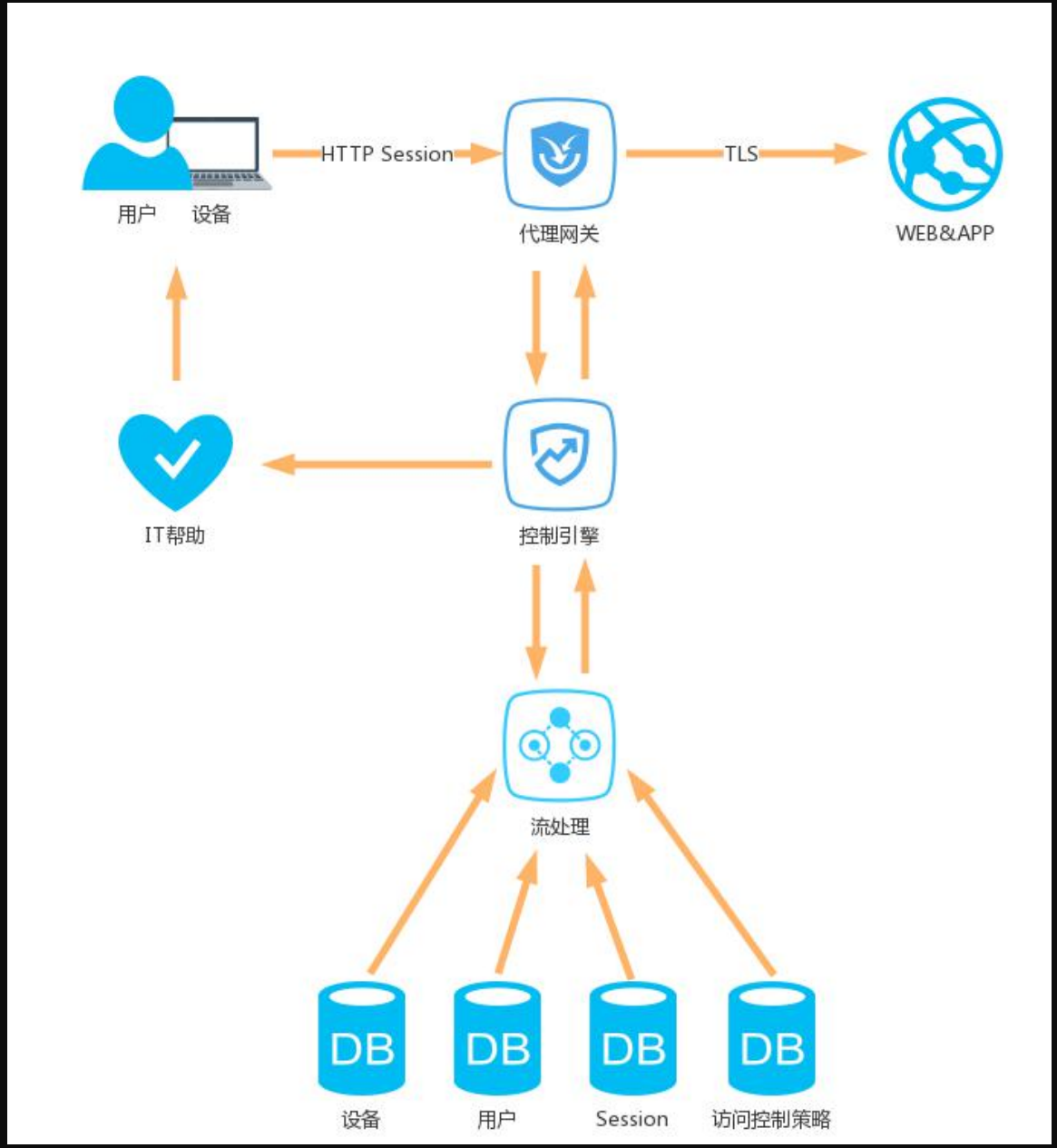
- 验证设备
- 验证用户
- 限制访问权限和特权
- 自学习和自适应

优点

- 重新定义身份，零信任模型通过状态组合动态实时评估。
- 集中控制，所有流量通过中央网关处理认证和授权。
- 主动防御，能够检查日志做审计和实时拦截主动防御是两回事。

# 一个端到端的示例

- 用户访问流程



# 总结

- 不依赖于内部网络分隔或防火墙作为我们的主要安全机制
- 最终用户登陆由中央服务器验证，然后中央服务器向用户端设备发送凭证，例如cookie或令牌，从客户端设备到Google的每个后续请求都需要该凭据。
- 使用应用程序级的访问管理控制，允许只在特定用户来自正确管理的设备以及期望的网络和地理位置时才将内部应用程序公开。
- 积极地限制和监督已经被授予基础设施管理权限的员工的活动，提供能安全和可控的方式完成相同任务的自动化，不断努力消除特定任务的特权访问需求。

# BeyondCorp 论文&QA



- 1、 BeyondCorp：企业安全新方法
  - https://static.googleusercontent.com/media/research.google.com/zh-CN//pubs/archive/43231.pdf
- 2、 BeyondCorp的设计和部署
  - https://static.googleusercontent.com/media/research.google.com/zh-CN//pubs/archive/44860.pdf
- 3、 代理
  - https://static.googleusercontent.com/media/research.google.com/zh-CN//pubs/archive/45728.pdf
- 4、 安全性和生产力
  - https://static.googleusercontent.com/media/research.google.com/zh-CN//pubs/archive/46134.pdf
- 5、 用户体验
  - https://storage.googleapis.com/pub-tools-public-publication-data/pdf/c8da594124dab1f91e6750995e2b7805403b19f1.pdf
- 6、构建运行良好的机组
  - https://storage.googleapis.com/pub-tools-public-publication-data/pdf/b9b4a09a913e410b7c45f3fbacec4d350e38146f.pdf

# Thanks

酷狗音乐 就是歌多